September 2024
Vol. XLIII, No 9

KEYSTONE MacCentral

printout

Keystone MacCentral Macintosh Users Group ❖ www.keystonemac.com

Keystone MacCentral September 17th Meeting

Please see your membership email for the links to this month's Zoom meeting or email us at KeystoneMacCentral@mac.com.

During our program this month we plan to discuss

- Recap September announcements

We have virtual meetings via Zoom on the third Tuesday of each month.

Emails will be sent out prior to each meeting. Follow the directions/invitation each month on our email – that is, just click on the link to join our meeting.

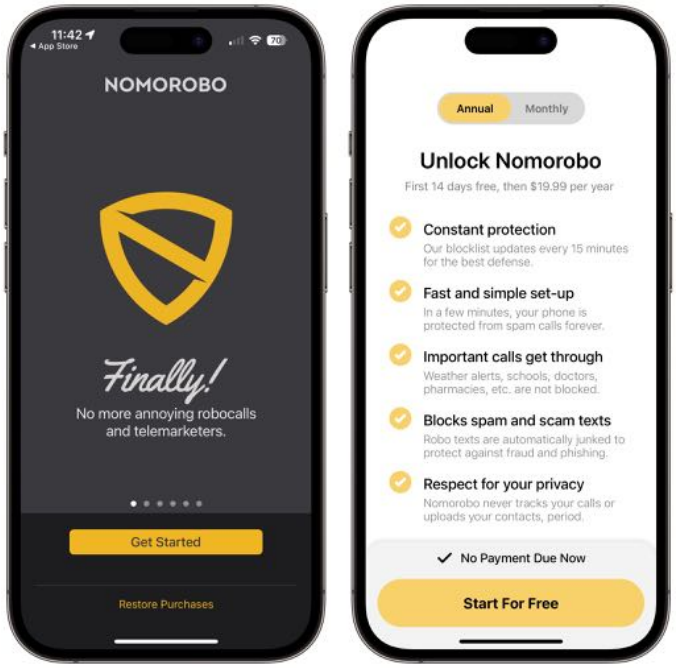
Contents

Keystone MacCentral is a not-for-profit group of Macintosh enthusiasts who generally meet the third Tuesday of every month to exchange information, participate in question-and-answer sessions, view product demonstrations, and obtain resource materials that will help them get the most out of their computer
systems. Meetings are free and open to the public. **The *Keystone MacCentral printout*** is the official newsletter of Keystone MacCentral and an independent publication not affiliated or otherwise associated with or sponsored or sanctioned by any for-profit organization, including Apple Inc.

By David Shayer

Block SMS Text Spam with Nomorobo

Have you been getting more SMS spam? If not, count yourself lucky, because my SMS spam load has gone through the roof recently. Apple's built-in option to filter unknown senders did what it promised but forced me to sort through all the texts from unknown senders for legitimate messages. I tried several SMS spam filters, none of which caught much of anything. Eventually, I settled on the longstanding call-protection service Nomorobo, which reined in the problem.



Spam Keeps Evolving

Years ago, email spam was a huge problem. There was an escalating war between spammers and spam filters. Eventually, spam filter technology won. Although email spam is still a thing, the vast majority of it is automatically filtered away. The main reason I use Gmail is its exemplary spam filtering. Those whose email provider isn't as good as Gmail can eliminate most spam with C-Command Software's venerable SpamSieve.

Then phone spam appeared. I received so many calls from telemarketers trying to sell me car warranties that I stopped answering calls from numbers I didn't recognize. Just as it seemed hopeless, Apple added the Silence Unknown Callers option (Settings > Phone > Silence Unknown Callers). Now calls from anyone not in my Contacts go straight to voicemail. Most spammers no longer leave voicemail; presumably, it's ineffective for whatever scam they're running. When a real person leaves me a voicemail, like my dentist confirming an appointment, I add that number to Contacts so they ring through the next time.

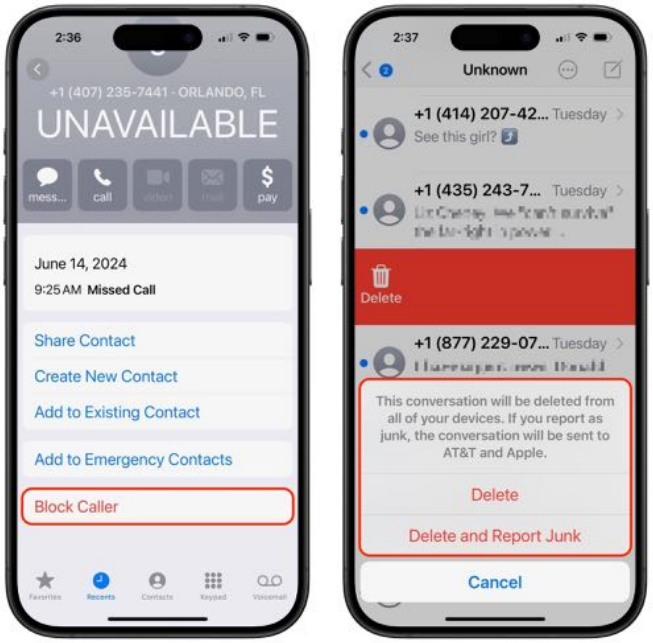
The latest spam frontier is SMS text spam. I used to receive a few spam texts, but now I may get a dozen a day. I get texts that an Amazon package I never ordered can't be delivered unless I click "amazon.scam.com/pkg/8675309" and sign in with my Amazon password. I get texts from "Jenny" asking, "Do you want some fun tonight?" But mostly I get texts from politicians asking for money. Somehow I've ended up on the lists for both US political parties. As the US election season heats up, the political spam is only getting worse.

Simple Solutions That Didn't Work

First, I figured I'd try Apple's built-in filtering. I turned on Settings > Messages > Filter Unknown Senders. That gives Messages a Filters link at the top left of the screen; tapping it reveals a list of filters that separate messages into Known Senders and Unknown Senders. Texts from numbers not in my Contacts appear in Unknown Senders, which sounds positive but proves relatively ineffective. The problem is that I still have to look through the Unknown Senders list for DoorDash orders, Uber confirmations, and two-factor authentication codes from numerous sites. Worse, some political spam texts appeared in Known Senders even though I don't have contacts for them.

Next, I tried blocking the phone numbers from which the spam texts originate. But each message comes from a unique number, presumably spoofed in many cases, which is easy to do. (I never tried replying to the actual scams.) I quickly accumulated hundreds of blocked numbers on my iPhone, but there was no reduction in spam texts.

For a while, I was religious about deleting spam texts and tapping Delete and Report Junk, but that doesn't seem to do anything. After months of reporting junk, I didn't notice any reduction in spam. I gather that reporting SMS text messages like this sends them to your carrier (you can also forward the messages to 7726), which can use the information to block similar spam texts. If the carriers actually do this, it's ineffective. With messages sent via iMessage, reporting them sends the information to Apple. I don't know anyone in the appropriate group at Apple, but other contacts in the company say they believe Apple uses the reports to help detect and revoke spammer accounts with enough reports.

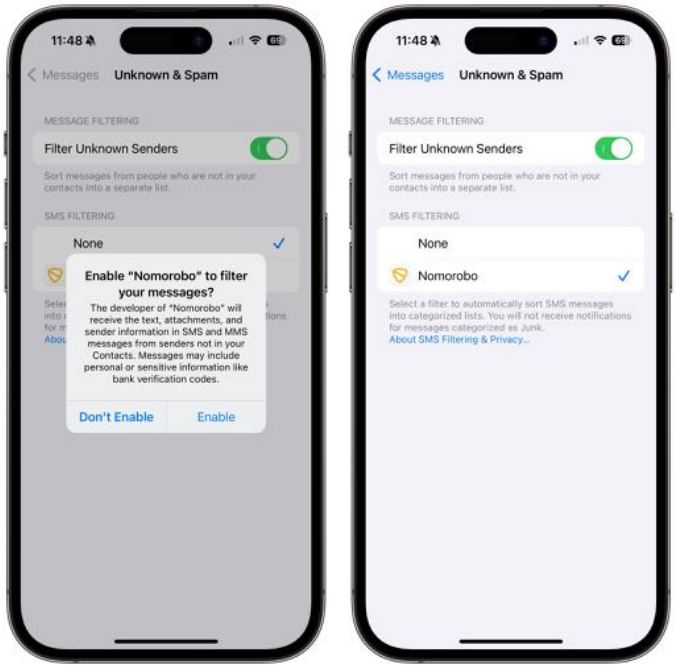


Some texts claim you can opt out by replying STOP, but I was reluctant to try this in many cases because it would confirm to a scammer that my number was live, possibly leading to even more text spam. Replying with STOP does work with political spam, but only with that particular candidate, so fighting political text spam becomes a game of Whac-A-Mole. Silence one candidate, and another pops up. (They're not even local!)

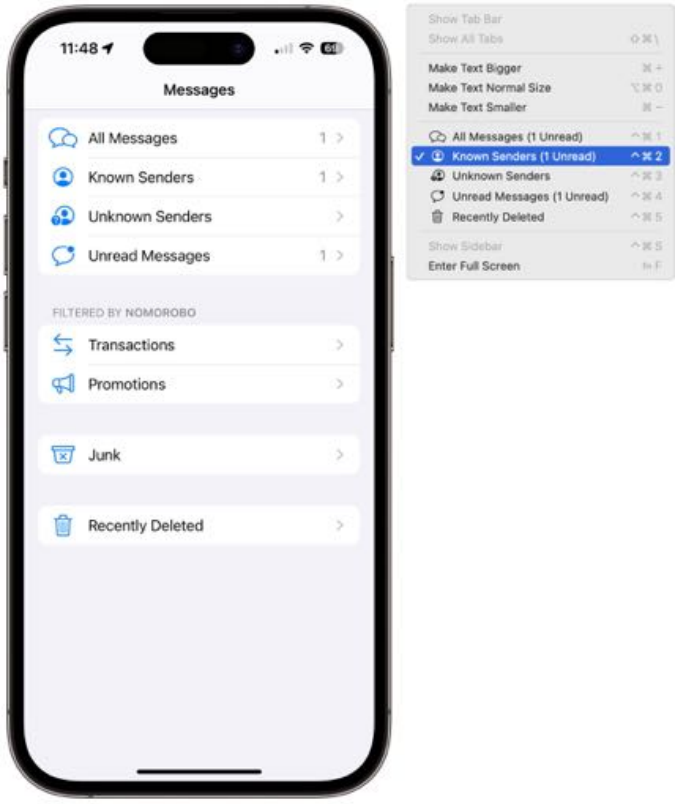
SMS Spam Filtering Apps

Surely there's an app for that. Next, I decided to try text spam filters. There are a bunch in the App Store that use Apple's official SMS and MMS Message Filtering API. Most of these filter apps require a subscription.

You install all these products similarly because they use Apple's API. Once you've downloaded one of these apps, go to Settings > Messages > Unknown & Spam, turn on Filter Unknown Senders, and select your SMS filtering app.



When you install a filtering app, the list of filters in Messages on your iPhone expands to include Transactions, Promotions, and Junk. If you have an iPad, Messages shows the same categories, and the messages are synced to them via iCloud Messages, which can sometimes stall for a few hours. The macOS version of Messages displays only the Known Senders and Unknown Senders lists in its View menu; messages filtered to the other groups are unavailable.



My testing was rather unscientific since I was primarily interested in solving my immediate problem. I used each spam filter on my own iPhone. Yes, that's a sample size of one, but they were all working in the same environment. Nor did I try every SMS filter in the App Store. Finally, most of these products block spam voice calls as well as spam texts, but I only tested the spam text feature—Silence Unknown Callers works well enough for me.

I don't mind paying for an SMS spam filtering app, but cost was still a factor. The winning app also had to work automatically and not make unnecessary requests for data, both of which turned out to be issues. Here are the apps I tried:

- **AT&T Active Armor:** Each of the major US cellular carriers (AT&T, T-Mobile, and Verizon) has a free spam filter in the App Store. AT&T's app is called AT&T Active Armor, Verizon has Verizon Call Shield iPhone, and T-Mobile offers T-Mobile Scam Shield. Verizon's and T-Mobile's apps only catch spam voice calls, not texts. Since I

use AT&T, I tested AT&T Active Armor. It caught only 5% of my spam texts.

- **Nomorobo:** Telephone Science Corporation, the company behind Nomorobo, is a decade old. Originally, the Nomorobo service blocked spam calls to landlines before expanding to protect cellular numbers from calls and then texts. After a 14-day free trial, Nomorobo costs $1.99 per month or $19.99 per year. The Nomorobo app identified 82% of my spam texts, placing them in the Junk list in Messages. That was far better than any of the other apps. It had no false positives—good texts identified as spam—but neither did the other apps.
- **Robokiller:** The Robokiller app offers a 7-day free trial, after which it costs between $4.99 and $7.99 per week or $39.99 to $149.99 per year, depending on which plan you buy. Robokiller would not activate without full access to my contacts, which I refused to give. There didn't seem to be any way around this, so I didn't go further with Robokiller.
- **SMS Spam Block:** Although the SMS Spam Block app is free, it is also fully manual and hasn't been updated in six years. You must set up a block list of disallowed words that filter out a message and an allow list that lets a message pass. I didn't test SMS Spam Block because I was looking for an automated solution.
- **TextKiller:** A separate app by the company behind RoboKiller, TextKiller also claims to block 99% of unwanted text messages. After a 7-day free trial, it costs $5.99 per month or $79.99 per year (which seems too high), between Nomorobo and Robokiller. The first time I tried TextKiller, the installation failed with an error message that seemed to indicate the company's server was down. When I tried again a few days later, it installed successfully. During testing, TetxtKiller turned off the setting to filter texts for no obvious reason, so I turned it back on. TextKiller filtered only 6% of my spam texts.

You can see why I stopped when I found Nomorobo, which was the cheapest and most effective of the commercial apps. AT&T Active Armor is free but ineffective. SMS Spam Block is also free but would have required me to maintain lists manually and hasn't been updated in six years. Robokiller triggered my alarm bells by refusing to activate without access to my contacts and was extremely expensive. TextKiller didn't instill confidence with its installation error and caught almost none of my spam.

If other text spam filtering apps have worked well for you, please share the details in the comments. But I'll be subscribing to Nomorobo. $20 per year is a small price to pay for eliminating a dozen text message interruptions per day.

By Adam Engst

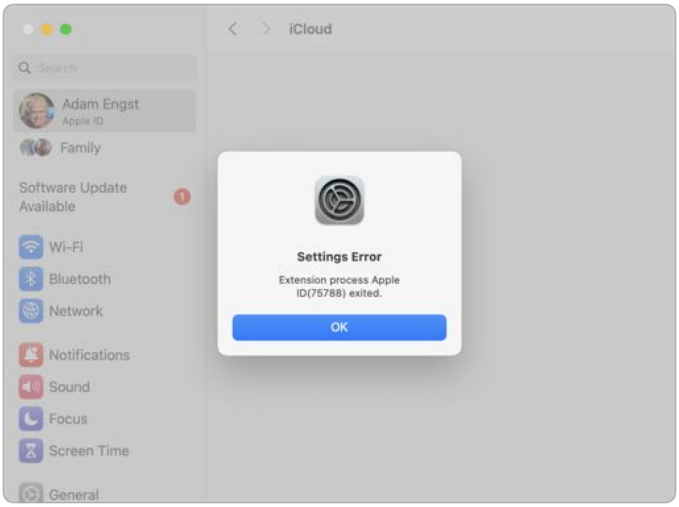
macOS 14.6.1, macOS 13.6.9, iOS 17.6.1, and iPadOS 17.6.1 Fix Advanced Data Protection

Apple had a bad week. On 29 July 2024, the company released updates to all its operating systems with a few minor changes in macOS 14.6 Sonoma and nothing but bug and security fixes for everything else (see "macOS 14.6 Enables Double Display Support for 14-inch M3 MacBook Pro," 30 July 2024). We noticed no problems after installing, so we gave our usual recommendation for minor updates that don't address zero-day security vulnerabilities—wait to install until it's convenient. Usually, showstopper problems will be reported within a few days, and Apple will pull

or replace the release quickly. This time, it took over a week.

On 7 August 2024, Apple pushed out macOS 14.6.1 Sonoma, iOS 17.6.1, and iPadOS 17.6.1 with release notes saying, "This update includes important bug fixes and addresses an issue that prevents enabling or disabling Advanced Data Protection." Apple also released macOS 13.6.9 Ventura with slightly more concise release notes that say, "This update addresses an issue that prevents enabling or disabling Advanced Data Protection." (For more information about what's involved here, see "Apple's Advanced Data Protection Gives You More Keys to iCloud Data," 8 December 2022.)

Indeed, when I went to System Settings > Your Name > iCloud > Advanced Data Protection and clicked the Turn On button, I was prompted for my Apple ID password, but the password dialog disappeared after I typed a single character, the System Settings screen flashed, and I was presented with the error below. On subsequent tries, the setup got farther, but I wasn't willing to remove my old devices from my account to complete the setup process.



Apple's security updates page says the updates don't address any vulnerabilities with CVE entries, and Howard Oakley reports that the only changes are to the Security framework and some keychain-related files. The question, then, is what might be included in those "important bug fixes."

There have been a small number of complaints about macOS 14.6. In TidBITS Talk, Ronald Lynch reported that, after updating to macOS 14.6, he lost access to Pages templates he had stored in the Template Chooser and couldn't create new ones. Installing macOS 14.6.1 didn't bring back his previously stored templates but allowed him to create new ones. In other forums, multiple people have reported extreme slowdowns and problems with Bluetooth pointing devices, plus individual complaints about mounted NAS volumes disappearing from the desktop and enterprise authentication issues. As yet, it's unclear if these were general bugs or issues specific to particular setups. Nor have follow-up posts said whether or not they were fixed by macOS 14.6.1.

iOS 17.6 has triggered complaints about dropped network connections and notifications not working, along with the perennial problems with battery life that usually resolve within a few days once iOS rebuilds indexes and caches. Again, I haven't seen any subsequent reports about iOS 17.6.1 either way.

There is one new complaint about macOS 14.6.1 related to headless Macs (those without displays). A TidBITS reader reported that he wasn't able to connect to a headless Mac mini after updating. He had to turn Remote Management off and back on to regain the ability to connect remotely. If you are updating a headless Mac, connect it to a keyboard, mouse, and display before updating, and toggle the Remote Management setting in System Settings > Sharing > Remote Management before removing them.

My revised advice about updating to this set of updates is as follows:

- If you're still running macOS 14.5, macOS 13.6.8, iOS 17.5, and iPadOS 17.5 with no problems, stick with them for a bit longer. None of the identified security vulnerabilities in those releases are actively being exploited in the wild, so there's no big win in updating right away. Revisit the question in a few weeks.
- If you updated to macOS 14.6, macOS 13.6.8, iOS 17.6, and iPadOS 17.6 but aren't having any

problems and don't intend to turn Advanced Data Protection on or off, stick with them for another week or two to make sure Apple didn't introduce any more bugs in the latest updates.

- If you updated to macOS 14.6, macOS 13.6.8, iOS 17.6, and iPadOS 17.6 and are having issues of any sort or want to turn Advanced Data Protection on or off, update right away to take advantage of Apple's fixes.

There's no question that Apple dropped the ball here. Advanced Data Protection may be a relatively new feature used by only a tiny percentage of the Apple audience, but automated testing should have caught the error I showed above. Perhaps Apple has redirected most of its testing resources to the forthcoming macOS 15 and iOS 18, but that's no excuse for causing trouble for the current user base with a weakly tested update.